CLAIMS

1.   A method for providing security for a computer network, comprising:

generating content sets for a computer associated with the network;

determining whether a user should be routed to the generated content sets;

5   selecting one of the content sets if it is determined that the user should be

routed to the generated content sets; and

routing the user to the selected generated content set.

2.   The method as recited in claim 1, further comprising monitoring the activities of

10   the user with respect to the computer.

3.   The method as recited in claim 2, further comprising preventing the user from

accessing files associated with said monitoring.

15 4.   The method as recited in claim 2, further comprising preventing the user from

accessing processes associated with said monitoring.

5.   The method as recited in claim 1, further comprising associating each generated

content set with a virtual computer.

20

6.   The method as recited in claim 5, wherein selecting one of the content sets

includes choosing a content set associated with a virtual computer requested to be

accessed by the user.

5   7.   The method as recited in claim 5, further comprising associating each generated

content set with its own network interface.

8.   The method as recited in claim 7, further comprising concealing from the user

network interfaces not associated with the selected generated content set.

10

9.   The method as recited in claim 5, further comprising concealing from the user

network connections not associated with the selected generated content set.

10.   The method as recited in claim 9, wherein concealing network connections

15   includes receiving a request from the user to access a network connection, checking

whether that network connection is associated with the selected generated content set,

and if it is not associated with the selected generated content set, providing an indication

that the network connection does not exist.

20   11.   The method as recited in claim 9, wherein concealing network connections

includes receiving a request from the user to access a network connection, checking

whether that network connection is associated with the selected generated content set,

and if it is not associated with the selected generated content set, transforming the request

into a request to access a network connection associated with the selected generated

content set.

12. The method as recited in claim 5, wherein the computer is running on a Unix

5   operating system.

13. The method as recited in claim 12, wherein the computer is running on a Solaris

operating system.

10   14. The method as recited in claim 1, wherein selecting one of the content sets

includes choosing a content set associated with a service requested to be accessed by the

user.

15. The method as recited in claim 14, wherein the service is telnet.

15

16. The method as recited in claim 1, wherein selecting one of the content sets

includes choosing a content set not currently in use by another user.

17. The method as recited in claim 1, further comprising storing the packets sent by

20   the user.

18. The method as recited in claim 1, further comprising logging information

concerning the files to which the user requests access.

19.   The method as recited in claim 1, further comprising preventing the user from

accessing content within the computer other than the selected generated content set.

5   20.   The method as recited in claim 1, further comprising screening a request by the

user to access a file to determine if access is permitted.

21.   The method as recited in claim 20, further comprising permitting access to a

requested file if it is determined that access to the requested file is permitted.

10

22.   The method as recited in claim 20, further comprising providing an indication that

a requested file does not exist if it is determined that access is not permitted.

23.   The method as recited in claim 1, further comprising generating additional content

15   subsequent to the step of generating content sets.

24.   The method as recited in claim 23, further comprising adding the additional

content to the selected generated content set.

20   25.   The method as recited in claim 1, wherein routing the user includes using network

address translation to route to the selected generated content set any user who requests to

access an unauthorized service.

26.   The method as recited in claim 25, wherein the unauthorized service is telnet.

27.   The method as recited in claim 1, further comprising receiving an indication that the user is no longer connected to the computer.

5

28.   The method as recited in claim 27, further comprising determining whether to retain changes in the files of the computer that resulted from the user's activities.

29.   The method as recited in claim 28, further comprising resetting the computer to

10   restore the computer and the selected generated content set to the condition they were in prior to the user being routed to the selected generated content set if it is determined the changes should not be retained.

30.   The method as recited in claim 29, further comprising updating the selected

15   generated content set by generating additional content that appears to have been created during a time period during which the user was connected to the computer.

31.   A method for providing security for a computer network, comprising:

        generating content sets for a file system for a first computer associated

20   with the network;

        creating a plurality of directories within the first computer;

        copying the file system of the first computer into each of the directories;

        and

routing a user who attempts to gain unauthorized access to a second

computer associated with the network to a first of the directories in the first

computer.

5   32.   The method as recited in claim 31, further comprising routing a user who attempts

to gain unauthorized access to a third computer associated with the network to a second

of the directories in the first computer.

33.   The method as recited in claim 31, further comprising associating at least one of

10   the directories with a virtual computer.

34.   The method as recited in claim 33, further comprising associating each virtual

computer with a network interface.

15   35.   A system for providing security for a computer network, comprising:

a computer configured to generate content sets for the computer, wherein

the computer is associated with the network;

a plurality of network interfaces each associated with one of the content

sets; and

20   a network device configured to determine whether a user should be routed

to the generated content sets, select one of the generated content sets if it is

determined that the user should be routed to the generated content, and to route

the user to the selected generated content set.

36.   The system as recited in claim 35, wherein the network device is a firewall.

37.   A computer program product for providing security for a computer network,

5   comprising a computer usable medium having machine readable code embodied therein for

generating content sets for a computer associated with the network;

determining whether a user should be routed to the generated content sets;

selecting one of the generated content sets if it is determined that the user

10   should be routed to the generated content sets; and

routing the user to the selected generated content set.

38.   A computer program product for providing multiple virtual computers on a

computer using a Solaris operating system, comprising a computer usable medium having

15   machine readable code embodied therein for

generating content sets for the computer, each generated content set

corresponding to a virtual computer;

allowing a user to access one of the generated content sets; and

preventing the user from detecting that the user is accessing a virtual

20   computer.